UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/066,252	01/31/2002	Massimiliano Antonio Poletto	12221-012001	2792

26161 7590 12/06/2007
FISH & RICHARDSON PC
P.O. BOX 1022
MINNEAPOLIS, MN 55440-1022

EXAMINER	
NALVEN, ANDREW L	
ART UNIT	**PAPER NUMBER**
2134	

MAIL DATE	DELIVERY MODE
12/06/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 10/066,252
Filing Date: January 31, 2002
Appellant(s): POLETTO ET AL.

Denis Maloney
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 25 September 2007 appealing from the Office action mailed 8 June 2007.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct. An after final amendment was submitted along with the instant appeal brief. The after final amendment has been entered.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is substantially correct.

Examiner has hereby withdrawn the rejection of claim 17 and thus claim 17 is hereby objected to as being dependent upon a rejected base claim.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

Mansfield et al, "Towards trapping wily intruders in the large", September 1999

2002/0083343	Crosbie et al	06-2002
2002/0069356	Kim	06-2002
2003/0084323	Gales	05-2003
7,162,737	Syvanne et al	01-2007

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claims 1, 5, 11, 24, 27 are rejected under 35 U.S.C. 102(a) as being anticipated by Mansfield "Towards trapping wily intruders in the large."

With regards to claim 1, Mansfield teaches a device, coupled to physical links between the data center and a network, with the device disposed to examine traffic entering or leaving that data center on the coupled physical links (Mansfield, page 6 Section 3.1, traffic monitors collect relevant packet count information from each link) and collect statistical information on packets that are sent between a network and the data center for a plurality of customers (Mansfield, page 6 Section 3.1, traffic monitors collect relevant packet count information from each link for multiple sites, Figure 4, sites 1, 2, 3, and 4) by examining traffic as if the device was disposed on links that are downstream from the links that the provisioned monitor is on (Mansfield, page 6 Section 3.1, traffic monitors traffic entering each site).

With regards to claims 5, Mansfield teaches the monitoring device being a data collector device (Mansfield, page 6 Section 3.1, traffic monitors collect relevant packet count information from each link for multiple sites).

With regards to claims 11, Mansfield teaches a provisioned monitor placed on selected links in the data center so that the provisioned monitor examines traffic entering or leaving the data center on the selected links (Mansfield, page 6 Section 3.1, traffic monitors collect relevant packet count information from each link) and collect statistical information for a plurality of provisioned customers which are on links that are downstream from links that the provisioned monitor is on (Mansfield, page 6 Section 3.1, traffic monitors collect relevant packet count information from each link for multiple sites, Figure 4, sites 1, 2, 3, and 4), the provisioned monitor maintaining separate counter logs for each provisioned customer (Mansfield, page 6, traffic monitor collects

information from link) and a global counter log that accounts for all traffic seen on the link that the provisioned monitor is coupled to (Mansfield, page 9, combines counts from probe 1 and probe 2 in Figure 8).

With regards to claim 24, Mansfield teaches collecting statistical information for a plurality of provisioned customers on links that are downstream from links on which collecting occurs (Mansfield, page 6 Section 3.1, traffic monitors collect relevant packet count information from each link for multiple sites, Figure 4, sites 1, 2, 3, and 4) and maintaining separate counter logs for each provisioned customer (Mansfield, page 6, traffic monitor collects information from link) and a global counter log that accounts for all traffic seen on the links on which collecting occurs (Mansfield, page 9, combines counts from probe 1 and probe 2 in Figure 8).

With regards to claim 27, Mansfield teaches collecting occurs on a data collector that samples network packets (Mansfield, page 6 Section 3.1, traffic monitors collect relevant packet count information from each link for multiple sites, Figure 4, sites 1, 2, 3, and 4) the data collector being disposed at a location that is at a large aggregation link in the network for the data center (Mansfield, Figure 6, probe monitors traffic entering network 1).

Claims 2-3, 7, 9-10, and 33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Mansfield "Towards trapping wily intruders in the large" in view of Crosbie et al US PGPub 2002/0083343.

With regards to claim 2, Mansfield fails to teach the monitoring device being coupled to a control center through a dedicated private network. However, Crosbie teaches the monitoring device being coupled to a control center through a dedicated private network (Crosbie, paragraph 0116-0118, SSL connection between management station and agent systems). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Crosbie's method of securing communication because it offers the advantage of preventing unauthorized modification or deletion of data as it flows across the network and helps detect when an interloper sends messages which purport to be from another machine (Crosbie, paragraph 0117).

With regards to claim 3, Mansfield as modified teaches a communication process that communicates statistics with the control center and which receives queries or instructions from the control center (Mansfield, page 6, NMS collects information from traffic monitors, page 10, agents can be accessed, queried, configured by security manager).

With regards to claim 7, Mansfield teaches collecting, using a provisioned monitor statistical information on packets that are sent between a network and a plurality of customers of the data center (Mansfield, page 6 Section 3.1, traffic monitors collect relevant packet count information from each link for multiple sites, Figure 4, sites 1, 2, 3, and 4) by examining traffic on selected links in the data center as if the collecting were being performed on links that are downstream from the selected links that the provisioned monitor is disposed on (Mansfield, page 6 Section 3.1, traffic monitors traffic entering each site). Mansfield fails to teach the communicating data over a

dedicated private network to a control center. However, Crosbie teaches the communicating data over a dedicated private network to a control center (Crosbie, paragraph 0116-0118, SSL connection between management station and agent systems). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Crosbie's method of securing communication because it offers the advantage of preventing unauthorized modification or deletion of data as it flows across the network and helps detect when an interloper sends messages which purport to be from another machine (Crosbie, paragraph 0117).

With regards to claims 9, Mansfield as modified teaches the monitoring device being a data collector device (Mansfield, page 6 Section 3.1, traffic monitors collect relevant packet count information from each link for multiple sites).

With regards to claim 10, Mansfield teaches the collecting occurring for inbound and outbound traffic (Mansfield, page 8, looks for reply messages, page 9, looks for request messages, Figure 8, incoming and outgoing).

With regards to claim 33, Mansfield teaches the control center determines a response to the attack (Mansfield, page 10, security manager uses network information to trap or track down intruder), but fails to teach communicating occurs on a downstream link basis over a dedicated, hardened network to a control center. However, Crosbie teaches communicating occurs on a downstream link basis over a dedicated, hardened network to a control center (Crosbie, paragraph 0116-0118, SSL connection between management station and agent systems). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize

Crosbie's method of securing communication because it offers the advantage of preventing unauthorized modification or deletion of data as it flows across the network and helps detect when an interloper sends messages which purport to be from another machine (Crosbie, paragraph 0117).

Claims 4, 6, 12-15, 25, 28-32, and 34 are rejected under 35 U.S.C. 103(a) as being unpatentable over Mansfield "Towards trapping wily intruders in the large" in view of Kim US PGPub 2002/0069356.

With regards to claim 4, Mansfield teaches a process to install filters to thwart denial of service attacks by removing network traffic that is deemed part of an attack (Mansfield, page 10, security manager uses network information to trap or track down intruder), but fails to teach the monitoring device is a gateway device. However, Kim teaches that the monitoring device is a gateway device (Kim, Abstract, integrated security gateway). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Kim's method of using a gateway because it offers the advantage of reducing costs by integrating security elements and increasing security by reducing the amount of elements that may be attacked (Kim, paragraphs 0012-0013).

With regards to claim 6, Mansfield as modified teaches a process to aggregate traffic from the various links and to produce logs and detection heuristics (Mansfield, page 9, combines counts from probe 1 and probe 2 in Figure 8).

With regards to claim 12, Mansfield teaches the provisioned monitor maintaining separate counter logs for each provisioned customer (Mansfield, page 6, traffic monitor collects information from link), but fails to teach the monitoring device is a gateway device. However, Kim teaches that the monitoring device is a gateway device (Kim, Abstract, integrated security gateway). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Kim's method of using a gateway because it offers the advantage of reducing costs by integrated security elements and increase security by reducing the amount of elements that may be attacked (Kim, paragraphs 0012-0013).

With regards to claim 13, Mansfield as modified teaches a global counter log that accounts for all traffic (Mansfield, page 9, combines counts from probe 1 and probe 2 in Figure 8).

With regards to claim 14, Mansfield as modified teaches the global counter includes a sample of all traffic seen on the link to which the gateway is connected (Mansfield, page 9, NMS combines counts from probe 1 and probe 2 in Figure 8, Kim, Abstract, integrated security gateway).

With regards to claim 15, Mansfield as modified teaches packet analysis for a particular virtual monitor happens by classifying packets based on addresses at the time of analysis (Mansfield, pages 5-6, source of malicious packet is traced).

With regards to claim 25, Mansfield teaches data collecting (Mansfield, page 6 Section 3.1, traffic monitors collect relevant packet count information from each link for multiple sites, Figure 4, sites 1, 2, 3, and 4), but fails to teach the monitoring device is a

gateway device located at the edge of a network. However, Kim teaches that the monitoring device is a gateway device (Kim, Abstract, integrated security gateway) located at the edge of a network (Kim, Figure 4 Item 420). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Kim's method of using a gateway because it offers the advantage of reducing costs by integrated security elements and increase security by reducing the amount of elements that may be attacked (Kim, paragraphs 0012-0013).

With regards to claim 28, Mansfield teaches performing intelligent traffic analysis and filtering to identify the malicious traffic and to eliminate malicious traffic (Mansfield, page 10, security manager uses network information to trap or track down intruder), but fails to teach the monitoring device is a gateway device. However, Kim teaches that the monitoring device is a gateway device (Kim, Abstract, integrated security gateway). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Kim's method of using a gateway because it offers the advantage of reducing costs by integrated security elements and increase security by reducing the amount of elements that may be attacked (Kim, paragraphs 0012-0013).

With regards to claim 29, Mansfield as modified teaches collecting statistical information for a plurality of links that are downstream from links on which collecting occurs (Mansfield, page 6 Section 3.1, traffic monitors collect relevant packet count information from each link for multiple sites, Figure 4, sites 1, 2, 3, and 4), performing traffic analysis on the collected statistical information on a per downstream link basis to

identify malicious traffic (Mansfield, page 6 Section 3.1, traffic monitors collect relevant packet count information from each link for multiple sites, Figure 4, sites 1, 2, 3, and 4), and communicating alerts that arise from the traffic analysis (Mansfield, pages 10-11, security manager is alerted to the detection of potential attempts).

With regards to claim 30, Mansfield as modified teaches the performing analysis occurs on statistical information collected for an individual one of the downstream links to identify malicious traffic intended for the individual one of the downstream links (Mansfield, page 6 Section 3.1, traffic monitors collect relevant packet count information from each link for multiple sites).

With regards to claim 31, Mansfield as modified teaches communicating to a control center occurs on a downstream link basis (Mansfield, page 9, combines counts from probe 1 and probe 2 in Figure 8).

With regards to claim 32, Mansfield as modified teaches communicating to a control center occurs on a downstream link basis Mansfield, page 9, combines counts from probe 1 and probe 2 in Figure 8) and the control center determines a response to the attack (Mansfield, page 10, security manager uses network information to trap or track down intruder).

With regards to claim 34, Mansfield teaches filtering the identified malicious traffic and to eliminate the malicious traffic from reaching the one of the downstream links (Mansfield, page 10, security manager uses network information to trap or track down intruder).

Claim 8 are rejected under 35 U.S.C. 103(a) as being unpatentable over Mansfield "Towards trapping wily intruders in the large" and Crosbie et al US PGPub 2002/0083343, as applied to claim 7 above, and in further view of Kim US PGPub 2002/0069356.

With regards to claim 8, Mansfield as modified teaches a process to install filters to thwart denial of service attacks by removing network traffic that is deemed part of an attack (Mansfield, page 10, security manager uses network information to trap or track down intruder), but fails to teach the monitoring device is a gateway device. However, Kim teaches that the monitoring device is a gateway device (Kim, Abstract, integrated security gateway). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Kim's method of using a gateway because it offers the advantage of reducing costs by integrated security elements and increase security by reducing the amount of elements that may be attacked (Kim, paragraphs 0012-0013).

Claims 16 is rejected under 35 U.S.C. 103(a) as being unpatentable over Mansfield "Towards trapping wily intruders in the large" and Kim US PGPub 2002/0069356, as applied to claim 13 above, and in further view of Gales US PGPub 2003/0084323.

With regards to claim 16, Mansfield as modified fails to teach the gateway maintaining duplicate packets keeping both a global packet log and a packet log for each virtual monitor. However, Gales teaches the gateway maintaining duplicate

packets keeping both a global packet log and a packet log for each virtual monitor (Gales, paragraph 0016, network activity log for information about global network usage, paragraph 0018, activity profile data has information for each of the nodes including inbound and outbound communication data). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Gales' method of keeping duplicate logs because it offers the advantage of allowing determination of security events on both a network and particular node level (Gales, paragraphs 0021-0022).

Claim 17 is rejected under 35 U.S.C. 103(a) as being unpatentable over Mansfield "Towards trapping wily intruders in the large" and Kim US PGPub 2002/0069356, as applied to claim 13 above, and in further view of Syvanne et al US Patent No. 7,162,737 and Gales US PGPub 2003/0084323.

With regards to claim 17, Mansfield as modified teaches a process to aggregate traffic from probes (Mansfield, page 9, combines counts from probe 1 and probe 2 in Figure 8) and to produce a global counter log and produce detection heuristics (Mansfield, page 9, combines counts from probe 1 and probe 2 in Figure 8, page 8, looks for reply messages, page 9, looks for request messages, Figure 8, incoming and outgoing) and a node head (Mansfield, page 9, combines counts from probe 1 and probe 2 in Figure 8). Mansfield as modified fails to teach producing a separate counter log for each provisioned customer or the gateway being a clustered gateway with a plurality of probes. However, Gales teaches the gateway maintaining

packet log for each virtual monitor (Gales, paragraph 0016, network activity log for information about global network usage, paragraph 0018, activity profile data has information for each of the nodes including inbound and outbound communication data). Syvanne teaches the gateway being a clustered gateway with a plurality of probes (Syvanne, column 5 line 60 – column 6 line 10, clustered gateway). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Syvanne's cluster methodology and Gale's logging method because it offers the advantage of allowing determination of security events on both a network and particular node level (Gales, paragraphs 0021-0022) and allows the flexible and reliable synchronization of state information between nodes in a gateway cluster (Syvanne, column 4 lines 50-60).

(10) Response to Argument

I. Mansfield anticipates all of the limitations of Claim 1

Applicant's argues that the cited references fail to teach all of the limitations of the claim 1. Specifically, Applicant argues on pages 11-12 that Mansfield fails to teach a device, coupled to physical inks between the data center and a network that collects statistical information on packets that are sent between the network and the data center for a plurality of customers as if the device was disposed on links that are downstream

from the links that the provisioned monitor is coupled to. Examiner respectfully disagrees.

Examiner contends that Mansfield teaches a device, coupled to physical links between the data center and a network, with the device disposed to examine traffic entering or leaving that data center on the coupled physical links and collect statistical information on packets that are sent between a network and the data center for a plurality of customers by examining traffic as if the device was disposed on links that are downstream from the links that the provisioned monitor is on.

First, Mansfield teaches a device, coupled to physical links between the data center and a network, with the device disposed to examine traffic entering or leaving that data center on the coupled physical links (Mansfield, page 6 Section 3.1, traffic monitors collect relevant packet count information from each link). Mansfield teaches the cited limitation by teaching traffic monitors disposed on network connections (Mansfield, Page 6, Figure 4). Each traffic monitor examines traffic entering or leaving sites (data centers) by collecting relevant packet count information from each link connecting each site/data center (Mansfield, Page 6, Section 3.1).

Second, Mansfield teaches collecting statistical information on packets that are sent between a network and the data center for a plurality of customers (Mansfield, page 6 Section 3.1, traffic monitors collect relevant packet count information from each link for multiple sites, Figure 4, sites 1, 2, 3, and 4). Mansfield teaches the cited limitation by teaching that each traffic monitor collects relevant packet count information from each link connected to each site (Mansfield, Page 6, Section 3.1). Mansfield's

traffic monitors examine traffic for each site/customer (Mansfield, page 6 Section 3.1, traffic monitors collect relevant packet count information from each link for multiple sites, Figure 4, sites 1, 2, 3, and 4). Thus, multiple customer sites in the form of data center sites are monitored by Mansfield's traffic monitors by way of the collection of statistical information.

Finally, Mansfield teaches that the collection of statistical information on packets occurs as if the device was disposed on links that are downstream from the links that the provisioned monitor is coupled to (Mansfield, page 6 Section 3.1, traffic monitors traffic entering each site). Mansfield teaches the cited limitation by teaching the traffic monitor disposed on the network link entering each site (Mansfield, Page 6, Figure 4). The traffic monitor collects packet count information from the link it is disposed on (Mansfield, page 6 Section 3.1, Figure 4). Because all packet count information for the link is collected including traffic entering and leaving the data center (see Mansfield, Page 7, Section 3.4, echo and response packets), Mansfield's traffic monitor acts as if it is disposed on links that are downstream. When data flows downstream from the sites the data flows out from a site into the network. Mansfield's traffic monitors collect packet count information on traffic on this link and thus Mansfield teaches that the collection of statistical information on packets occurs as if the device was disposed on links that are downstream from the links that the provisioned monitor is coupled to.

II. Mansfield anticipates all of the limitations of Claims 11, 24, and 27

Applicant's argues that the cited references fail to teach all of the limitations of the claims 11, 24, and 27. Specifically, Applicant presents arguments similar to those noted above with regards to claim 1 and further asserts that Mansfield fails to teach that the provisioned monitor maintains separate counter logs for each provisioned customer and a global counter log that accounts for all traffic seen on the link that the provisioned monitor is coupled to. Examiner respectfully disagrees. For Applicant's arguments similar to those regarding claim 1 please see Examiner's response above.

Mansfield teaches that the provisioned monitor maintains separate counter logs for each provisioned customer and a global counter log that accounts for all traffic seen on the link that the provisioned monitor is coupled to. Mansfield teaches the provisioned monitor maintaining separate counter logs for each provisioned customer (Mansfield, page 6, traffic monitor collects information from link) and a global counter log that accounts for all traffic seen on the link that the provisioned monitor is coupled to (Mansfield, page 9, combines counts from probe 1 and probe 2 in Figure 8). Mansfield teaches the cited limitation by teaching that each traffic monitor separately collects packet count statistics on the link on which it is disposed (Mansfield, page 6 Section 3.1, traffic monitors collect relevant packet count information from each link). Thus, each monitor has a counter log that it maintains that pertains to each individual customer viewed by the Examiner as a site (Mansfield, Page 6, Figure 4, sites 1, 2, 3, 4). Mansfield teaches a global counter log that accounts for all traffic seen on the link by disclosing the combining of the counts from each traffic monitor that pertain to each

site/customer (Mansfield, page 9, combines counts from probe 1 and probe 2 in Figure 8).

III. The combination of Mansfield and Crosbie anticipate all of the limitations of Claims 2, 3, 7, 9, 10, and 33

Applicant's argues that the cited references fail to teach all of the limitations of the claims 2, 3, 7, 9, 10, and 33. Specifically, Applicant argues that Mansfield and Crosbie fail to teach the monitoring device being coupled to a control center through a dedicated private network. Examiner respectfully disagrees.

Mansfield fails to teach the monitoring device being coupled to a control center through a dedicated private network. However, the deficiencies of Mansfield are remedied by Crosbie. Crosbie teaches the monitoring device being coupled to a control center through a dedicated private network (Crosbie, paragraph 0116-0118) by teaching an SSL connection between a management station and agent systems. Crosbie's management station corresponds to the claimed control center and Crosbie's agent systems correspond to the claimed monitoring devices. The SSL connection between the management station and agent systems meets the limitation of a dedicated private network because SSL provides a secure point to point connection between two stations. A secure point to point connection is a dedicated private network because a network is any combination of computer elements and in this case the network is dedicated to secure transmission of data between two predefined entities. Hence, Crosbie's SSL

connection providing a secure dedicated connection between an IDS system (monitoring device) and the management station (Crosbie, paragraph 0118) meets the limitation of the monitoring device being coupled to a control center through a dedicated private network.

Regarding Applicant's further arguments towards claims 7, 9, and 10 on page 17 see Examiner's remarks above with regards to claims 1 and 11.

IV. The combination of Mansfield and Kim anticipate all of the limitations of Claims 4, 6, 12-15, 25, 28-32, and 34

Applicant's argues that the cited references fail to teach all of the limitations of the claims 4, 6, 12-15, 25, 28-32, and 34. Specifically, Applicant argues that Mansfield and Kim fail to teach a gateway including a process to install filters to thwart denial of service attacks. Examiner respectfully disagrees.

Regarding claim 4 and all claims dependent therefrom, Mansfield teaches a process to install filters to thwart denial of service attacks by removing network traffic that is deemed part of an attack (Mansfield, page 10, security manager uses network information to trap or track down intruder), but fails to teach the monitoring device is a gateway device. However, Kim remedies the deficiencies of Mansfield by teaching that a gateway device can be used as a monitoring device that installs filters (Kim, Abstract, integrated security gateway). Kim's gateway device acts to install filters in order to respond to security issues . While Kim's device is not specifically directed to thwarting

denial of service attacks the principle is the same. Kim's gateway filters packets and allows packets that are permissible and denies packets that violate packet filtering rules (Kim, paragraphs 0031-0033). Thus, Examiner maintains that all of the limitations of claim 4 are met where Kim teaches the use of a gateway to install filters and Mansfield teaches a process to thwart denial of service attacks. One of ordinary skill in the art would have been motivated to use Kim's method of using a gateway for packet filtering because it offers the advantage of reducing costs by integrating security elements and increasing security by reducing the amount of elements that may be attacked (Kim, paragraphs 0012-0013). Thus, through the use of Kim's gateway based method, multiple devices such as gateways, proxies, and monitoring devices may be integrated into a single unit which would reduce the cost and complexity of a network. Examiner maintains that a prima facie case of obviousness has been made.

Regarding claims 6 and 12-15, see Examiner's remarks above regarding claims 4 and 11 and the aggregation of separate counter logs into a global counter log.

Regarding claim 25, the combination of Mansfield and Kim teach a gateway as noted above and further teach that the gateway is disposed at an edge of the network (Kim, Figure 4 Item 420). Kim teaches a gateway disposed at the edge of a network by teaching an Integrated Security Gateway (Kim, Figure 4 Item 420) placed between an internal network (Kim, Figure 4 Item 410) and the Internet (Kim, Figure 4 Item 450).

Regarding claims 29, 30-32 and 34, see Examiner's remarks above regarding claims 1 and 11.

V. The combination of Mansfield, Crosbie and Kim anticipate all of the limitations of Claim 8

Applicant's argues that the cited references fail to teach all of the limitations of the claim 8. Examiner respectfully disagrees. Please see the above remarks regarding claims 1 and 4 for Examiner's response.

VI. The combination of Mansfield, Gales and Kim anticipate all of the limitations of Claim 16

Applicant's argues that the cited references fail to teach all of the limitations of the claim 16. Examiner respectfully disagrees. Please see the above remarks regarding claims 4 and 11 for Examiner's response.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

Andrew Nalven

KAMBIZ ZAND
SUPERVISORY PATENT EXAMINER

Conferees:

Kambiz Zand

KAMBIZ ZAND
SUPERVISORY PATENT EXAMINER

Kim Vu